RELIANCE - YIPES

AGREEMENT

THIS AGREEMENT (the "**Agreement**") is made as of the Effective Date, by and between the following:

Reliance Communications Limited ("**Reliance Communications**"), and its subsidiary

Reliance Gateway Net Limited ("**Reliance Gateway**") (collectively "**Reliance**"),

FLAG Telecom Group Limited ("**FLAG Group**"), which is wholly owned by Reliance, and its subsidiary

FLAG Telecom Group Services ("**FLAG Services**") (collectively "**FLAG**"),

(Reliance and FLAG, collectively, the "**Acquirer**");

Yipes Holdings, Inc. ("**Yipes Holdings**") and its subsidiary

Yipes Enterprise Services, Inc. ("**Yipes Services**") (collectively "**Yipes**"),

(the Acquirer and Yipes, collectively, the "**Communications Service Providers**"), on behalf of themselves and all current and future affiliates and subsidiaries, and

the U.S. Department of Justice ("**DOJ**"), and

the U.S. Department of Homeland Security ("**DHS**"),

(the "**USG Parties**")

(referred to individually as a "**Party**" and collectively as the "**Parties**").

RECITALS

WHEREAS, the Parties undertake this Agreement based upon the following recitals:

(1) U.S. communication systems are essential to the ability of the U.S. Government to fulfill its responsibilities to the public to preserve the national security of the United States, to enforce the laws, and to maintain the safety of the public;

(2) the U.S. Government has an obligation to the public to ensure that U.S. communications and related information are secure in order to protect the privacy of U.S.

persons, to enforce the laws, and to protect the national security of the United States;

(3) it is critical to the well being of the Nation and its citizens to maintain the viability, integrity, and security of the communications systems of the United States (see e.g., Executive Order 13231, Critical Infrastructure Protection in the Information Age, and Homeland Security Presidential Directive / HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection);

(4) preventing the disruption and preserving the integrity of communications in the U.S. and preventing the unauthorized dissemination to Foreign Persons and Foreign Entities, including foreign governments, of certain information and technology is critical to preserving the national security of the United States;

(5) protection of Classified Information and Sensitive Information is also critical to U.S. national security;

(6) the Acquirer, a Foreign Entity, is a global provider of communications services;

(7) Yipes Services currently provides to the financial, legal, government (Federal state, and local), educational, and healthcare industries managed Ethernet and application delivery services, including common carrier transport services, via a network of more than 22,000 route kilometers of fiber and associated equipment across seventeen (17) major U.S. metropolitan markets;

(8) Yipes Services operates two (2) Network Operations Centers (NOCs) in the United States in Denver, Colorado, and San Francisco, California, and, in addition to its seventeen (17) domestic markets, has existing Points of Presence (POPs) in London, United Kingdom (U.K.), Tokyo, Japan, and Hong Kong, Peoples Republic of China, and is in the process of deploying additional POPs in Frankfurt, Germany, Toronto, Canada, and London, U.K.;

(9) Yipes Services has integrated its communications network with various global partners as well as major U.S. telecommunications common carriers and Internet service providers (ISPs);

(10) Yipes Services also has access to a certain customer and end-user information that is subject to U.S. privacy and electronic surveillance laws;

(11) Yipes Services has an obligation under U.S. law to protect from unauthorized disclosure the contents and Transactional Data of communications transiting its network as well as customer and end-user information;

1.5 "**Classified Information**" shall have the meaning indicated in Executive Order 12958, as amended by Executive Order 13292, or any successor executive order, or the Atomic Energy Act of 1954, or any statute that succeeds or amends the Atomic Energy Act of 1954.

1.6 "**Control**" and "**Controls**" means the power, direct or indirect, whether or not exercised, and whether or not exercised or exercisable through the ownership of a majority or a dominant minority of the total outstanding voting securities of an entity, or by proxy voting, contractual arrangements, or other means, to determine, direct, or decide matters affecting an entity; in particular, but without limitation, to determine, direct, take, reach, or cause decisions regarding:

(a) the sale, lease, mortgage, pledge, or other transfer of any or all of the principal assets of the entity, whether or not in the ordinary course of business;

(b) the dissolution of the entity;

(c) the closing and/or relocation of the production or research and development facilities of the entity;

(d) the termination or nonfulfillment of contracts of the entity;

(e) the amendment of the articles of incorporation or constituent agreement of the entity with respect to the matters described in Section 1.6(a) through (d); or

(f) the obligations of the Communications Service Providers under this Agreement.

1.7 "***De facto***" and "***de jure***" control have the meanings provided in 47 C.F.R. § 1.2110.

1.8 "**Domestic Communications**" means: (a) Wire Communications or Electronic Communications (whether stored or not) from one U.S. location to another U.S. location; and (b) the U.S. portion of a Wire Communication or Electronic Communication (whether stored or not) that originates or terminates in the United States, in each case where such Wire Communications or Electronic Communications are transmitted (in whole or in part) via the Domestic Communications Infrastructure.

1.9 "**Domestic Communications Infrastructure**" means: (a) transmission, switching, bridging and routing equipment (including software and upgrades) used by or on behalf of Yipes to provide, process, direct, control, supervise or manage Domestic Communications; (b) facilities and equipment used by or on behalf of Yipes physically located in the United States; and (c) facilities to control the equipment described in (a) and (b) above, but does not include entities with which the Communications Service Providers have contracted for peering, interconnection, roaming, long distance, or other similar arrangements on which the Parties may agree, nor

equipment or facilities used by service providers other than Yipes that are interconnecting communications providers.

1.10 "**Domestic Network Management Information**" means network management operations plans, processes and procedures; descriptions of the placement of NOC(s) and linkages (for service offload or administrative activities) to other domestic and international carriers, ISPs and other critical infrastructures; descriptions of networks and operations processes and procedures for management control and relation to the backbone infrastructure(s) including other service providers; description of any unique or proprietary control mechanisms as well as operating and administrative software; and network performance information.

1.11 "**Effective Date**" means the date this Agreement becomes effective, which is the date this Agreement is signed by the last Party to sign it (as indicated by the date stated opposite that Party's signature).

1.12 "**Electronic Communication**" has the meaning given it in 18 U.S.C. § 2510(12).

1.13 "**Electronic Surveillance**," for the purposes of this Agreement, includes: (a) the interception of wire, oral, or electronic communications as defined in 18 U.S.C. §§ 2510(1), (2), (4) and (12), respectively, and electronic surveillance as defined in 50 U.S.C. § 1801(f); (b) Access to stored wire or electronic communications, as referred to in 18 U.S.C. § 2701 *et seq.*; (c) acquisition of dialing, routing, addressing, or signaling information through pen register or trap and trace devices or other devices or features capable of acquiring such information pursuant to law as defined in 18 U.S.C. § 3121 *et seq.* and 50 U.S.C. § 1841 *et seq.*; (d) acquisition of location-related information concerning a service subscriber or facility; (e) preservation of any of the above information pursuant to 18 U.S.C. § 2703(f); and (f) Access to, or acquisition, interception, or preservation of, wire, oral, or electronic communications or information as described in (a) through (e) above and comparable state laws.

1.14 "**FCC Application**" includes all information whether in oral or written form provided to the FCC or any agency of the U.S. Government in connection with that application.

1.15 "**Foreign**" where used in this Agreement, whether capitalized or lower case, means non-U.S.

1.16 "**Foreign Person**" means any Person who is not a U.S. Person as provided by 31 C.F.R. § 800.222.

1.17 "**Foreign Entity**" means any Foreign Person, any Entity established under the laws of a country other than the United States, or any government other than the U.S. Government or a U.S. state or local government.

1.18 "**Government**," "**Government Authority**," or "**Government Authorities**" means any government, or any governmental, administrative, or regulatory entity, authority, commission, board, agency, instrumentality, bureau or political subdivision and any court, tribunal, judicial or arbitral body.

1.19 "**Intercept**" or "**Intercepted**" has the meaning defined in 18 U.S.C. § 2510(4).

1.20 "**Lawful U.S. Process**" means lawful U.S. federal, state, or local Electronic Surveillance or other court orders, processes, or authorizations issued under U.S. federal, state, or local law for physical search or seizure, production of tangible things, or Access to or disclosure of Domestic Communications, Transactional Data, or Subscriber Information.

1.21 "**Management of Yipes**" means its officers and members of the Board of Directors.

1.22 "**Network Operations Center**" or "**NOC**" means the facilities and equipment used to monitor, secure, maintain, configure, or operate communications, data, supervisory control and data acquisition ("SCADA"), or business management networks or equipment for Domestic Communications and the Domestic Communications Infrastructure.

1.23 "**NOC Services**" means 24x7 NOC or network management, network flow and/or monitoring services provided on behalf of the Communications Service Providers in support of Domestic Communications and the Domestic Communications Infrastructure.

1.24 "**NOC Services Personnel**" means all Personnel performing NOC Services wherever located.

1.25 "**Personnel**" means (i) employees, officers, directors, and agents and (ii) contract or temporary employees (part-time or full-time) who are under the direction or control of Yipes; provided, however, that "Personnel" does not include independent contractors, customers, customers' agents, and vendors who are not employed by or operate under the direction or control of Yipes.

1.26 "**Screened Positions**" are those Personnel positions that

(a) allow Access to the Domestic Communications Infrastructure and enables such persons in fact or potentially to monitor the content of Wire or Electronic Communications (including in electronic storage) and/or direct any form of such communications to an unauthorized recipient;

(b) allow Access to Transactional Data;

(c) allow Access to Sensitive Information;

(d) perform NOC Services; or

(e) perform security services.

1.27 "**Security Officer**" means the Head of Security for Yipes, or a designee in a direct reporting relationship with the Head of Security, who serves as the Security Officer with the primary responsibility for ensuring compliance with the Communications Service Providers' obligations under this Agreement.

1.28 "**Sensitive Information**" means information that is not Classified Information regarding: (a) the persons or facilities that are the subjects of Lawful U.S. Process; (b) the identity of the Government Authority or Government Authorities serving such Lawful U.S. Process; (c) the location or identity of the line, circuit, transmission path, or other facilities or equipment used to conduct Electronic Surveillance; (d) the means of carrying out Electronic Surveillance; or (e) the type(s) of service, telephone number(s) or other similar identifiers, records, communications, or facilities subjected to Lawful U.S. Process; as well as all other information that is not Classified Information but is designated in writing by an authorized official of a federal, state, or local law enforcement agency or a U.S. intelligence agency as "Sensitive Information" of some type recognized by the agency involved. The designation "Sensitive" as used in this Section includes but is not limited to information marked or labeled "Official Use Only," "Limited Official Use Only," "Law Enforcement Sensitive," "Sensitive Security Information," "Sensitive but Unclassified," "Controlled Unclassified Information," or other similar designations.

1.29 "**Subscriber Information**" means all records or other information relating to customers or subscribers of Yipes of the type referred to and Accessible subject to procedures specified in 18 U.S.C. § 2703(c) or (d) or 18 U.S.C. § 2709. Such information shall also be considered Subscriber Information when it is sought pursuant to the provisions of other Lawful U.S. Process.

1.30 "**Transactional Data**" includes the following when associated with a Domestic Communication but does not include the content of any communication:

(a) "call identifying information," as defined in 47 U.S.C. § 1001(2), including without limitation the telephone number or similar identifying designator;

(b) any information related to the sender or recipient of that Domestic Communication, including, without limitation subscriber identification, called party number, calling party number, start time, end time, call duration, feature invocation and deactivation, feature interaction, registration information, user location, diverted to number, conference party numbers, post-cut-through dialed digit extraction, in-band and out-of-band signaling, and party add, drop and hold;

(c) any information relating specifically to the identity and physical address of a customer or subscriber, or account payer, or the end-user of such customer or subscriber, or account payer, or associated with such person relating to all telephone numbers, domain names, Internet Protocol ("**IP**") addresses, Uniform Resource Locators ("**URLs**"), other identifying designators, types of services, length of service, fees, usage including billing records and connection logs, and the physical location of equipment, if known and if different from the location information provided under (e) below;

(d) the time, date, size, or volume of data transfers, duration, domain names, Media Access Control ("**MAC**") or IP addresses (including source and destination), URL's, port numbers, packet sizes, protocols or services, special purpose flags, or other header information or identifying designators or characteristics, including electronic mail headers showing From: and To: addresses; and

(e) as to any mode of transmission (including mobile transmissions), and to the extent permitted by U.S. laws, any information indicating as closely as possible the physical location to or from which a Domestic Communication is transmitted.

1.31 "**United States**" or "**U.S.**" means the United States of America, including all of its States, districts, territories, possessions, commonwealths, and the special maritime and territorial jurisdiction of the United States.

1.32 "**Visitor**" means any Person who enters a Yipes facility other than Personnel.

1.33 "**Wire Communication**" has the meaning given it in 18 U.S.C. § 2510(1).

1.34 **Other Definitional Provisions**. Other capitalized terms used in this Agreement and not defined in this Article shall have the meanings assigned them elsewhere in this Agreement. The definitions in this Agreement are applicable to the singular as well as the plural forms of such terms and to the masculine as well as to the feminine and neuter genders of such term. Whenever the words "include," "includes," or "including" are used in this Agreement, they shall be deemed to be followed by the words "without limitation."

ARTICLE 2: FACILITIES, INFORMATION STORAGE AND ACCESS

2.1 **Domestic Communications Infrastructure**. Except to the extent and under conditions concurred in by the USG Parties in writing:

(a) all Domestic Communications Infrastructure shall be directed, controlled, supervised and managed by Yipes exclusively from within the United States; and

(b) Yipes shall provide technical or other assistance upon lawful request to facilitate Electronic Surveillance pertaining to the Domestic Communications Infrastructure.

2.2 **NOCs**. With respect to NOCs on the Domestic Communications Infrastructure or otherwise having access to Domestic Communications, the Communications Service Providers agree as follows:

(a) Yipes shall provide written notice to the USG Parties at least **thirty (30) days** prior to activating any new NOC on the Domestic Communications Infrastructure or decommissioning any NOC existing as of the Effective Date;

(b) NOC Services Personnel located outside the United States shall not exercise control of U.S. network elements of the Domestic Communications Infrastructure, and if an event occurs that requires escalation or intervention, U.S.-based NOC Services Personnel shall address such event; provided, that NOC Services Personnel located outside the United States may address such event only with the oversight and direct authorization of U.S.-based NOC Services Personnel;

(c) Yipes shall prevent unauthorized changes to any network flow or configuration of the Domestic Communications Infrastructure through NOC Services or other means.

2.3 **Compliance with Lawful U.S. Process**. The Communications Service Providers agree that Yipes shall take all practicable steps to configure the Domestic Communications Infrastructure to be capable of complying, and Yipes employees in the United States will have unconstrained authority to comply, in an effective, efficient, and unimpeded fashion, with:

(a) Lawful U.S. Process;

(b) the orders of the President of the United States in the exercise of his/her authority under § 706 of the Communications Act of 1934, as amended, (47 U.S.C. § 606), and under § 302(e) of the Aviation Act of 1958 (49 U.S.C. § 40107(b)) and Executive Order 11161 (as amended by Executive Order 11382); and

(c) National Security and Emergency Preparedness rules, regulations and orders issued pursuant to the Communications Act of 1934, as amended (47 U.S.C. § 151 *et seq.*).

2.4 **Information Storage and Access**. Unless otherwise agreed to by the Parties, Yipes shall store exclusively in the United States the following:

(a) Domestic Communications, if such communications are stored by or on behalf of Yipes for any reason;

(b) Transactional Data, if such communications are stored by or on behalf of Yipes for any reason;

(c) Subscriber Information, if such communications are stored by or on behalf of Yipes for any reason;

(d) Billing Records of domestic customers or subscribers of Yipes, if such communications are stored by or on behalf of Yipes for any reason; and

(e) Domestic Network Management Information, if such communications are stored by or on behalf of Yipes for any reason.

Notwithstanding the foregoing, nothing in this Section imposes any restriction on storage of Yipes account information, which shall include information relating to invoicing, collections and customer service used in the ordinary course of business. Furthermore, nothing in this Section is meant to exclude the use of Yipes Transactional Data for business or network management purposes in the normal course of business if said data is subject to security and access controls. The phrase "on behalf of" as used in this Section does not include entities with which Yipes contracts in the ordinary course of business for peering, interconnection, roaming, collocation, long distance, or other similar commercial arrangements.

2.5 **Storage Pursuant to 18 U.S.C. § 2703(f)**. Upon a request made pursuant to 18 U.S.C. § 2703(f) by a Government Authority within the United States to preserve any information in the possession, custody, or control of Yipes, including any information that is listed in Section 2.4 above, Yipes shall store such preserved records or other evidence in the United States.

2.6 **Compliance with U.S. Law**. Nothing in this Agreement shall excuse the Communications Service Providers from any obligation they may have to comply with U.S. legal requirements for the retention, preservation, or production of information, records or data as well as all applicable requirements of CALEA, as applicable by law.

ARTICLE 3: SECURITY

3.1 **Security Officer.** Within **ten (10) business days** of the Effective Date, Yipes shall designate a Security Officer to act as the point of contact to the USG Parties regarding compliance with this Agreement and any national security issues.

(a) The Security Officer shall

(i) be a resident U.S. citizen corporate officer of Yipes;

(ii) hold a U.S. security clearance or meet the criteria that would be considered in a security clearance process; and

(iii) possess the authority to enforce this Agreement.

(b) The Communications Service Providers shall consult in advance of the designation of the Security Officer with the USG Parties and shall reasonably address any concerns raised by the USG Parties regarding the selection and identity of the Security Officer.

(c) The Security Officer shall have access to all information necessary to perform his or her duties, including, without limitation, security-related and technical information and business information, including but not limited to information regarding the existing and emerging products and services of Yipes and business plans of the Communications Service Providers affecting Yipes' ability to perform its obligations under this Agreement.

(d) If any action of the Security Officer to enforce compliance with this Agreement is blocked or denied or the relevant information under this Agreement is not provided for any reason, the Security Officer shall immediately (not to exceed **five (5) days** from acquiring actual notice) report that fact to the USG Parties.

3.2 **Continuation of Current Level of Security Standards**. Yipes shall take all reasonable measures to maintain its security standards and policies at no less than the level represented to the USG Parties as of the Effective Date.

3.3 **Measures to Prevent Improper Use or Access**. Yipes shall take all reasonable measures to prevent the use of or Access to the Domestic Communications Infrastructure to conduct Electronic Surveillance, or to Access, obtain or disclose Domestic Communications, Transactional Data, Subscriber Information, Sensitive Information, in violation of any U.S. federal, state, or local laws or the terms of this Agreement. These measures shall include maintaining and/or creating and complying with written policies and procedures related to a comprehensive security strategy for Domestic Communications and the Domestic Communications Infrastructure, including all related activities of the Communications Services Providers. Upon written request of the USG Parties (or any of them), these policies and procedures shall be made available to the requesting Party or Parties. Furthermore, Yipes agrees to meet and confer with the USG Parties and reasonably address any concerns they may raise as part of the procedure described herein.

3.4 **Access by Foreign Government Authorities**. Notwithstanding the provisions of Article 2.4 above, the Communications Service Providers shall not, directly or indirectly, disclose or permit disclosure of, or provide Access to Domestic Communications, Transactional Data, or Subscriber Information, stored by or on behalf of Yipes to any person if the purpose of such Access is to respond to legal process or the request of or on behalf of a Foreign Government, identified representative, component or subdivision thereof, without the express written consent of the USG Parties or the authorization of a court of competent jurisdiction in the United States. Any such requests or submission of legal process shall be reported to the USG Parties as soon as possible and in no event later than **ten (10) business days** after such request or legal process is received by or known to Yipes. Yipes shall take reasonable measures to ensure that they will promptly learn of all such requests or submission of legal process.

3.5 **Disclosure to Foreign Government Authorities**. Yipes shall not, directly or indirectly, disclose or permit disclosure of, or provide Access to:

(a) Sensitive Information;

(b) Transactional Data, Subscriber Information, or a copy of any Wire or Electronic Communications, intercepted or acquired pursuant to Lawful U.S. Process; or

(c) the existence of Lawful U.S. Process that is not already a matter of public record;

to any Foreign Government, identified representative, component or subdivision thereof, without satisfying all applicable U.S. federal, state and local legal requirements, and without obtaining either the express written consent of the USG Parties or the authorization of a court of competent jurisdiction in the United States. Any requests or any legal process submitted by a Foreign Government, an identified representative, a component or subdivision thereof to Yipes for the communications, data or information identified that is maintained by Yipes shall be referred to the USG Parties as soon as possible and in no event later than **ten (10) business days** after such request or legal process is received by or known to Yipes, unless the disclosure of the request or legal process would be in violation of an order of a court of competent jurisdiction within the United States. Yipes shall take reasonable measures to ensure that it will promptly learn of all such requests or submission of legal process.

3.6 **Notification of Access or Disclosure Requests from Foreign Non-Governmental Entities**. Within **ten (10) business days** after receiving legal process or requests from Foreign non-governmental entities for Access to or disclosure of Domestic Communications, Yipes shall notify the USG Parties in writing of such legal process or requests, unless such disclosure would be in violation of an order of a court of competent jurisdiction within the United States.

3.7 **Security of Lawful U.S. Process**. Yipes shall protect the confidentiality and security of all Lawful U.S. Process served upon it and the confidentiality and security of Sensitive